
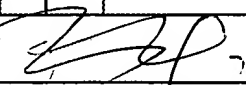


FORM PTO-1449 (REV. 7-80)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY. DOCKET NO. NIT-294		SERIAL NO.	
LIST OF DOCUMENTS CITED BY APPLICANT <i>(Use several sheets if necessary)</i>				APPLICANT M. KAMINAGA et al			
				FILING DATE August 29, 2001		GROUP	
U.S. PATENT DOCUMENTS							
* EXAMINER INITIAL	AA	DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE <i>(If Appropriate)</i>
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES NO
	AL						<input type="checkbox"/> <input type="checkbox"/>
	AM						<input type="checkbox"/> <input type="checkbox"/>
	AN						<input type="checkbox"/> <input type="checkbox"/>
	AO						<input type="checkbox"/> <input type="checkbox"/>
	AP						<input type="checkbox"/> <input type="checkbox"/>
OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, etc.)</i>							
30	AR	SMART CARD HANDBOOK, p. 263					
20	AS	Tamper Resistance - a Cautionary Note, pp. 1-11.					
20	AT	Chinese Remaindering Based Cryptosystems in the Presence of Faults, pp. 1-5.					
EXAMINER <i>[Signature]</i>				DATE CONSIDERED <i>9/26/05</i>			

* EXAMINER Initial If reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

FORM PTO-1449 (REV. 7-80)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY. DOCKET NO. NIT-294		SERIAL NO.	
LIST OF DOCUMENTS CITED BY APPLICANT <i>(Use several sheets if necessary)</i>				APPLICANT M. KAMINAGA et al			
				FILING DATE August 29, 2001		GROUP	
U.S. PATENT DOCUMENTS							
* EXAMINER INITIAL		DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE <i>(If Appropriate)</i>
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	<div style="display: flex; justify-content: space-between;"> <div>TRANSLATION</div> <div>YES</div> <div>NO</div> </div>
	AL						<input type="checkbox"/> <input type="checkbox"/>
	AM						<input type="checkbox"/> <input type="checkbox"/>
	AN						<input type="checkbox"/> <input type="checkbox"/>
	AO						<input type="checkbox"/> <input type="checkbox"/>
	AP						<input type="checkbox"/> <input type="checkbox"/>
OTHER DOCUMENTS <i>(Including Author, Title, Date, Pertinent Pages, etc.)</i>							
	AR	Modular Multiplication Without Trial Division:, P. Montgomery, pp. 519-521.					
	AS						
	AT						
EXAMINER 				DATE CONSIDERED 9/26/05			
<small>* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.</small>							



Sheet 1 of 2

FORM PTO-1449 (REV. 7-80)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY. DOCKET NO. NIT-294		SERIAL NO. 09/940,985	
LIST OF DOCUMENTS CITED BY APPLICANT (Use several sheets if necessary)				APPLICANT M. KAMINAGA et al			
				FILING DATE August 29, 2001		GROUP 2137	
U.S. PATENT DOCUMENTS							
* EXAMINER INITIAL		DOCUMENT	DATE	NAME	CLASS	SUBCLASS	FILING DATE (If Appropriate)
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
FOREIGN PATENT DOCUMENTS							
		DOCUMENT	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES NO
30	AL	0946018	09/1999	EUROPE			<input type="checkbox"/> <input type="checkbox"/>
30	AM	WO 00/42511	07/2000	PCT			<input type="checkbox"/> <input type="checkbox"/>
20	AN	WO 99/63696	12/1999	PCT			<input type="checkbox"/> <input type="checkbox"/>
	AO						<input type="checkbox"/> <input type="checkbox"/>
	AP						<input type="checkbox"/> <input type="checkbox"/>
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)							
30	AR	"A Timing Attack against RSA with the Chinese Remainder Theorem", Werner Schindler, CHES 2000, LNCS 1965, pp. 109-124.					
	AS						
EXAMINER 26 Zachary Davis				DATE CONSIDERED 9/26/05			
* EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.							